REMARKS

In the Office Action, the Examiner objected to claims 9, and 10, 12, 14, 23, 24, 38, 39, and 44 for various informalities. The Examiner rejected claims 47 and 48 under 35 USC § 102(e) as being anticipated by Morar (i.e., U.S. Patent No. 6,678,822). The Examiner rejected claims 7 - 9, 11 - 13, 23, 38 - 44, and 50 - 54 under 35 USC § 103(a) as being unpatentable over Morar in view of Kaufman (U.S. Patent No. 5,497,421). The Examiner also rejected claims 10, 14, 24, 25, 45, and 49 under 35 USC § 103(a) as being unpatentable over Morar in view of Kaufman and Schneier ("Applied Cryptography", second edition, 1996, pages 193 - 194). The Examiner also rejected claim 46 under 35 USC § 103(a) as being unpatentable over Morar in view of Kaufman, further in view of Zubeldia (US Patent 6,397,224). The Applicant has amended independent claim 7 by incorporating the language recited in claim 9, which is hereby canceled. The Applicant has amended the language of former claim 9, claims 10, 12, 14, 23, and 24 others to correct the informalities and thereby tend to the Examiner's objections. The Applicant, however, believes the language recited in claims 38, 39, and 49 is clear and definite. Without specific objections to these claims, the Applicant has chosen to not amend these claims.

Claims 7 - 13

In amended claim 7, the Applicant recites a method for de-identification of records that includes, among other things, selecting at least a portion of formatted personal identification data fields and determining if the selected portion of personal identification data fields is to be encoded. If the selected portion of the formatted personal identification data fields is to be encoded, then that portion is encoded and the remaining personal identification data fields (i.e., the personal identification data fields that are not selected) are deleted. After encoding the selected portion of the formatted personal identification data fields, they are one-way encrypted.

The Examiner stated in his rejection that Morar teaches encrypting the selected personal identification data fields at column 11, lines 63 through 65. The Examiner also stated that Morar discloses determining if the selected personal identification data fields are to be encoded and then encoding those personal identification data fields (i.e., in the rejection of former claim 9) at column 8, line 55 to column 9, line 53 and column 11, lines 37 through 65. While Morar does appear to teach many alternatives with respect to sanitizing information of certain items, Morar does not teach a method that includes both encoding and encrypting. For example, Morar

generally discusses obscuring private information by means of a replacement process (e.g., that removes the private information or otherwise replaces it with other information or encrypts it). However, Morar does not teach a step of obscuring private information that is followed by a step of encrypting the unsecured private information. In this regard, Morar does not teach or reasonably suggest that which the Applicant claims. Nor does Kaufman supplement Morar to teach or reasonably suggest a step of encoding personal identification data fields followed by a step of encrypting the encoded personal identification data fields. Accordingly, claim 7 is novel and non-obvious in view of the cited references. The Applicant, therefore, respectfully requests reconsideration and allowance of claim 7.

Claims 8 and 10 - 13 depend from independent claim 7 and inherit all of the novel and non-obvious features of the independent claim. However, these claims require additional features that further distinguish from the cited references. For example, in claim 13, the Applicant recites a step concatenating at least a portion of each of the first encryption result and the second encryption result for each of the encoded portion of the formatted personal identification data fields to respectively provide binary string identifiers for the encoded portion of the formatted personal identification data fields. Claim 13 also requires a step of converting the binary strings to alphanumeric strings to provide match codes. The Examiner states that Kaufman discloses one-way encrypting that includes a step of concatenating at least a portion of each of the first encryption result and the second encryption result for the data to respectively provide binary string identifiers for the data at column 6, lines 37 - 58. Here, Kaufman describes a process in which first and second hash totals, H1 and H2, are computed. The hash total H1 is then used to encrypt a user's private RSA key to form an “encrypted credential”. The encrypted credential is then appended to the hash total H2 to form a "doubly encrypted credential". In other words, Kaufman teaches a process that appends a hash total to an encrypted result. Kaufman's process, however, does not concatenate first and second encrypted portions of personal identification data fields to respectively provide binary string identifiers for the encoded portion of the formatted personal identification data fields. The Examiner also states that Morar teaches converting the binary strings to alphanumeric strings to provide match codes at column 7, lines 31 through 39. Here, Morar appears to teach a process of evaluating files, programs, etc. to determine whether they are infected with bugs or undesirable software (e.g., viruses). But, Morar does not teach a conversion of binary strings to alphanumeric strings to provide match

codes as the Applicant claims. Since neither Morar nor Kaufman teach or reasonably suggest that which the Applicant claims, claim 13 is novel and non-obvious in view of the cited references. The Applicant, therefore, respectfully requests reconsideration and allowance of claim 13.

Claim 14

In claim 14, the Applicant recites a method for de-identification of records that includes, among other things, a step of encoding a selected portion of personal identification data fields and concatenating the encoded portion of the personal identification data fields with a seed value to provide seed value identifiers. The seed value identifiers are then first one-way encrypted with a first encryption algorithm and second one-way encrypted with a second encryption algorithm. The method further includes concatenating at least a portion of each one-way encryption result from the first one-way encrypting and the second one-way encrypting corresponding to the seed value identifiers to respectively provide binary strings for each of the seed value identifiers. The method also includes converting the binary strings to alphanumeric strings to provide match codes. The de-identified records include the match codes and are created at the programmed client computer prior to transmission to a server computer.

Regarding the encoding step followed by the one-way encrypting steps with first and second encryption algorithms, the Applicant has addressed such in the arguments for patentability of claim 7. Regarding the step of concatenating to provide binary strings for each of the seed value identifiers and the step of converting the binary strings, the Applicant has addressed such in the arguments for patentability of claim 13. Regarding the de-identified records including match codes that are created a program client computer prior to transmission to a server computer, neither Morar nor Kaufman teacher reasonably suggest such match codes. The match codes of the Applicant's claims are used for linking de-identified records at the server computer (see e.g., page 4, column 14 of the present application). The Examiner states and such is taught by Morar at column 9, line 54 to column 10 line 4 and at column 12, lines 31 - 46. The Applicant respectfully disagrees because, here, Morar simply teaches filtering macros and/or data in a manner that is consistent with the sanitization of Morar. For example, Morar refers to macros as executable software modules that may be removed and placed into a suspect information container prior to transmission. See e.g., column 9, lines 14 - 20 and, lines 54 – 59

of Morar. This is not analogous to the match codes as the Applicant claims because, among other reasons, the match codes are included (i.e. not removed) from the de-identified records. At column 12, Morar teaches the exchange of an encryption key. The encryption key, however, does not appear to link any records (e.g., replace any previously removed records). Encryption keys, like Morar teaches at column 12, lines 42 through 44, simply unencrypt previously encrypted data. The Applicant believes the match codes of claim 14 patently distinguish in view of the cited references. For at least these reasons, the Applicant maintains that claim 14 is novel and non-obvious in view of the cited references. The Applicant, therefore, respectfully requests reconsideration and allowance of claim 14.

Claim 23

In claim 23, the Applicant recites a computer readable media containing a program which, when executed by a programmed client computer, causes execution of a method. The executed method has been amended to recite the same claim limitations recited in claim 7. The arguments in favor of patentability for claim 7 apply herein well. The Applicant respectfully requests reconsideration and allowance of claim 23.

Claim 24

The Examiner rejected claim 24 for the same reasons recited in claim 14 stating that claim 24 is a computer readable medium claim that corresponds to method claim 14 and is, therefore, rejected for the same reasons. Since claim 24 is of a similar scope with respect to claim 14, the arguments in favor of patentability for claim 14 apply herein as well. Accordingly, the Applicant respectfully requests reconsideration and allowance of claim 24.

Claim 25 depends from claim independent 24 and inherits all of the novel and non-obvious features of the independent claim. However, claim 25 requires additional novel and non-obvious features that further distinguish from the cited references. For at least these reasons, the Applicant believes claim 25 is in condition for allowance and respectfully requests such disposition.

Claims 38 – 46

In claim 38, the Applicant recites a method for de-identification of records that includes,

among other things, deleting a first portion of parsed personal identification data fields and one-way encrypting a second portion of parsed personal identification data fields to generate one or more de-identified records. As similarly discussed in the arguments for patentability of claim 7, Morar appears to teach many alternatives with respect to sanitizing information of certain items, such as obscuring private information by means of replacement or removal. However, Morar does not teach a method that includes both deleting (e.g., removing) and encrypting. In this regard, Morar does not teach or reasonably suggest that which the Applicant claims. Nor does Kaufman supplement Morar to teach or reasonably suggest a step of deleting a first portion of parsed personal identification data fields followed by a step of one-way encrypting a second portion of parsed personal identification data fields to generate one or more de-identified records. Accordingly, claim 38 is novel and non-obvious in view of the cited references. The Applicant, therefore, respectfully requests reconsideration and allowance claim 38.

Claims 39 through 46 depend from independent claim 38 and inherit all of the novel and non-obvious features of the independent claim. For at least these reasons, claims 39 through 46 are also novel and non-obvious in view of the cited references. However, these claims recite additional subject matter that further distinguish from the cited references. For example, claim 40 for recites that the method further comprises concatenating the personal identification data fields that are one-way encrypted with the seed value to provide seed value identifiers. The Examiner has stated that neither Morar nor Kaufman teach such a process of concatenation but that Schneier does on page 194. Here, Schneier teaches a method of using an interference vector that is used to encrypt a first block of data. The encrypted first block of data is then used as an interference vector for the encryption of the second block of data. However, Schneier does not teach *concatenating* a personal identification data fields with a seed value. Accordingly, Schneier does not teach that which the Applicant claims. The Applicant, therefore, respectfully requests reconsideration and allowance of claim 46.

Claims 47 – 53

In claim 47, the Applicant recites a system for de-identifying records that includes a client computer having an interface for receiving records. The client computer is adapted to locate personal identification data fields in the records, delete at least a portion of the personal

identification data fields, and encrypt remaining personal identification data fields to generate encrypted personal identification data fields. As similarly recited in the arguments for patentability of claim 7, Morar appears to teach many alternatives with respect to sanitizing information of certain items, such as obscuring private information by means of replacement or removal. However, Morar does not teach a method that includes both deleting (e.g., removing) and encrypting. In this regard, Morar does not teach or reasonably suggest that which the Applicant claims. Accordingly, claim 47 is novel and non-obvious in view of the cited references. The Applicant, therefore, respectfully requests reconsideration and allowance claim 47.

Claims 48 through 53 depend from independent claim 47 and inherit all of the novel and non-obvious features of the independent claim. For at least these reasons, claims 48 through 53 are also novel and non-obvious in view of the cited references. However, these claims require additional features that further distinguish from the cited references. For example, in claim 52, the Applicant recites a first encryption result that comprises concatenation of a least a portion of each of the first encryption result and the second encryption result for each of the personal identification data fields to respectably provide binary string identifiers for the personal identification data fields. In claim 53, the Applicant recites that the binary strings are converted to alphanumeric strings to provide match codes. The limitations of each of these claims were similarly recited in claim 13. As such, the arguments in favor of patentability for claim 13 apply to claims 52 and 53 as well. The Applicant, therefore, respectfully requests reconsideration and allowance of claims 52 and 53, as well as claims 48 through 51.

Claim 54

Claim 54 recites a system for de-identification of records comprising means of a similar scope recited in claim 38. The Examiner rejected claim 54 for the same reasons recited in claim 38 stating that claim 54 corresponds to method claim 38 and is rejected for the same reasons. Since claim 54 is of a similar scope with respect to claim 38, the arguments in favor of patentability for claim 54 apply herein as well. Accordingly, the Applicant respectfully requests reconsideration and allowance of claim 54.

CONCLUSION

In view of the above, the Applicant believes that all claims are in condition for allowance and respectfully requests such disposition. In the event that a telephone conversation would further prosecution and/or expedite allowance, the Examiner is invited to contact the undersigned.

Respectfully submitted,

MARSH FISCHMANN & BREYFOGLE LLP

By: /GREGORY T. FETTIG/
Gregory T. Fettig
Registration No. 50,843
3151 South Vaughn Way, #411
Aurora, CO 80014
(720) 562-5509

Date: 09-07-06